ARMY RESEARCH LABORATORY

The Methodology Process Flow of a SLAD Information Systems Survivability Assessment

by Richard L. zum Brunnen

ARL-TR-1747 August 1998

Army Research Laboratory
Aberdeen Proving Ground, MD 21010-5423

ARL-TR-1747 **August 1998**

The Methodology Process Flow of a SLAD Information Systems Survivability Assessment

Richard L. zum Brunnen
Survivability/Lethality Analysis Directorate, ARL

Abstract

The Information Systems Survivability Assessment (ISSA) is a process of analytical steps that the Survivability/Lethality Analysis Directorate (SLAD) of the U.S. Army Research Laboratory (ARL) applies to networked Automated Information Systems (INFOSYS) of military interest.

The ISSA Plan for a particular system is a focused plan that has been designed to provide the decision-makers the necessary information with which to make informed decisions concerning the vulnerabilities and susceptibilities of the system to Information Operations (IO) threats. The ISSA is a multiple-phase effort; these phases are intertwining tasks. Each of these tasks depends upon the others.

The plan is formulated in various phases to help the decision-makers modify the necessary hardware and software within the program cycle to meet the necessary survivability requirements. The ISSA culminates with protection measures being recommended to identify and minimize the impact of the IO threats on system performance. By addressing the IO threats, the system will significantly improve its survivability by planning for both the avoiding and withstanding of potential problems with IO-based threats.

This report discusses the ISSA process in detail and shows how each small task dovetails into the larger effort.

Table of Contents

INTENTIONALLY LEFT BLANK.

List of Figures

List of Tables

INTENTIONALLY LEFT BLANK.

1. An Overview of Information Systems Survivability (ISS)

The Information Systems Survivability Assessment (ISSA) is a process of analytical steps that the Survivability/Lethality Analysis Directorate (SLAD) of the U.S. Army Research Laboratory (ARL) applies to networked, automated information systems (INFOSYS) of military interest. INFOSYS are defined here as defined in both Joint Pub 6-0 [1] and FM 100-6 [2].

- INFOSYS from Joint Pub 6-0: The entire infrastructure, organization, personnel, and components that collect, process, store, transmit, display, disseminate, and act on information.

- INFOSYS from FM 100-6: INFOSYS allow the commander to view and understand his battle space, communicate his intent, lead his forces, and disseminate his pertinent information throughout his chain of command and his area of operation. Effective military and nonmilitary INFOSYS help the staff get the right information to the right location in time to allow commanders to make quality decisions and take appropriate actions.

This discussion focuses primarily on the ISS as defined in VAL-CE-TR-92-22 [3].

- ISS from VAL-CE-TR-92-22: The ability of a computer-communication-system-based application to continue satisfying its requirements (for example, requirements for security, reliability, real-time responsiveness, and correctness) in the face of adverse conditions.

The goal of SLAD's ISS tools, techniques, and methodology (TTM) development program is to generate predictive computer models that predict, as closely as is reasonably possible, the real-world-observed behavior of specific information processor properties caused by various real-world stimuli using an agreed-upon set of metrics. These stimuli range from normal network operations to the stressing stimuli caused by various software errors, hardware errors, and the multitude of the different forms of intentional or unintentional misuse and hostile attacks to which an information processor may be subjected.

Figure 1 [4] shows the overall schema of the modeling approach that will be taken to achieve this goal. Models are based on data that are obtained through real-world observations, measurements, assumptions, approximations, and predictions. These data are distilled using verified algorithms into model parameters, both variable inputs and fixed coefficients. The modeler/analyst perceives the structure of real-world events and converts this perception to a symbolic representation, through the use of a computer language, into a computer model. Interpretation, verification, and modification are some of the events used by the modeler/analyst to adjust the symbolic representation. There are several attributes, which the modeler/analyst can possess, that are useful in balancing the observed behavior of the real world with the model behavior. These are experience; intuition; and a knowledge base of the primary, and a great many of the secondary, academic disciplines. These disciplines include physics, computer science, optics, mathematics, statistics, electronics, etc.

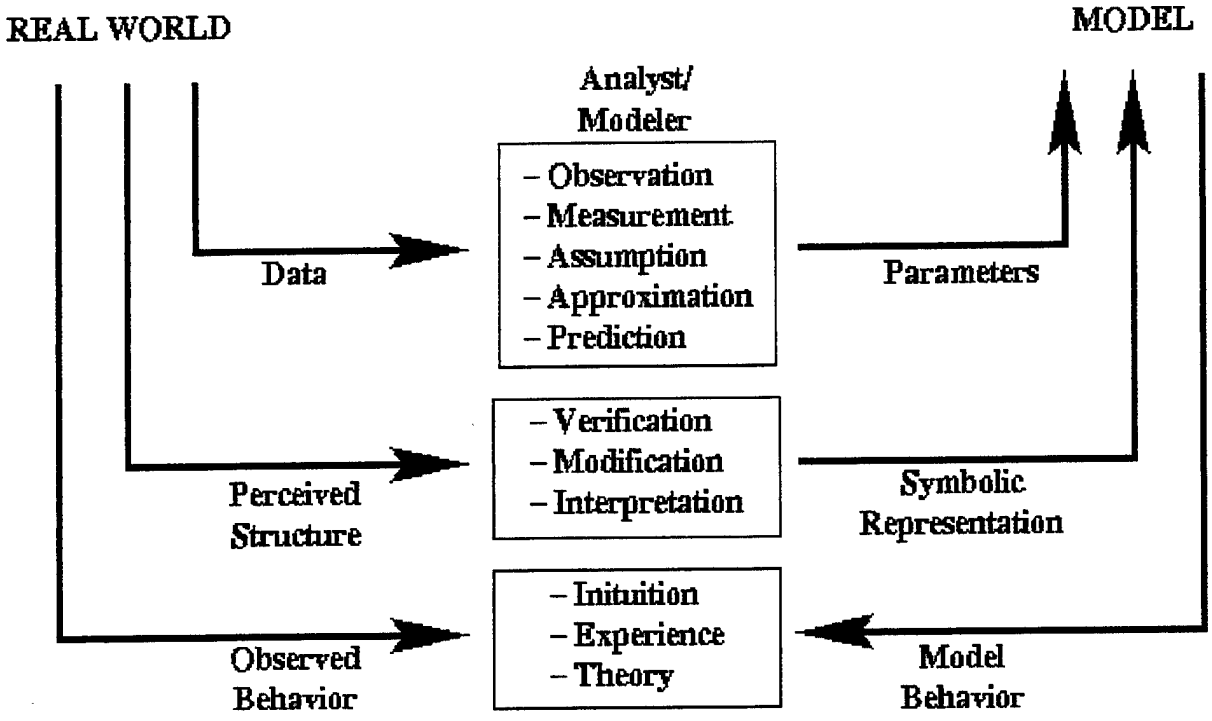

Figure 1. System Modeling.

Classes of models range from simple, look-up tables (in two or more dimensions) to the complex task of predicting the outcomes of live-fire shoots. Simulations may be an amalgamation of numerous individual models from multiple classes.

Analyses preformed by SLAD are concerned with an extremely broad spectrum of threats. The classification of these threats include ballistic, nuclear, chemical, electronic, atmospheric, and information based. SLAD has historical backgrounds in all of these threats. The information-based threats are relativity new threats and have become a concern with the advent of information processors (computer systems) on the battlefield.

An element of SLAD's mission is to conduct integrated analysis. This is a scenario-based analysis containing the occurrence of two or more separate threats. The primary guide used by SLAD for these integrated analyses is the vulnerability/lethality (V/L) taxonomy. This V/L taxonomy has been documented and enhanced in numerous reports [5–21] and is depicted in Figure 2. As pointed out in Ruth and Hanes [20], the integration of the separate threat effects happens in the V/L taxonomy with the mapping between level 2 (damage state) and level 3 (capability state). This mapping is typically performed using fault trees. For the integration of separate threat analyses to be successful, the desire for an integrated product has to be a primary design consideration in any analytical process. Compatibility and conformance with the SLAD-integrated product was an objective motivating the design of the SLAD ISSA presented herein.

2. The ISSA Process

The ISSA is structured in five phases, as shown in Table 1. Each of these five phases has its own procedures and connects to the following phases through particular products. The flow, interconnection, and the products passing through these five phases are shown in Figure 3.

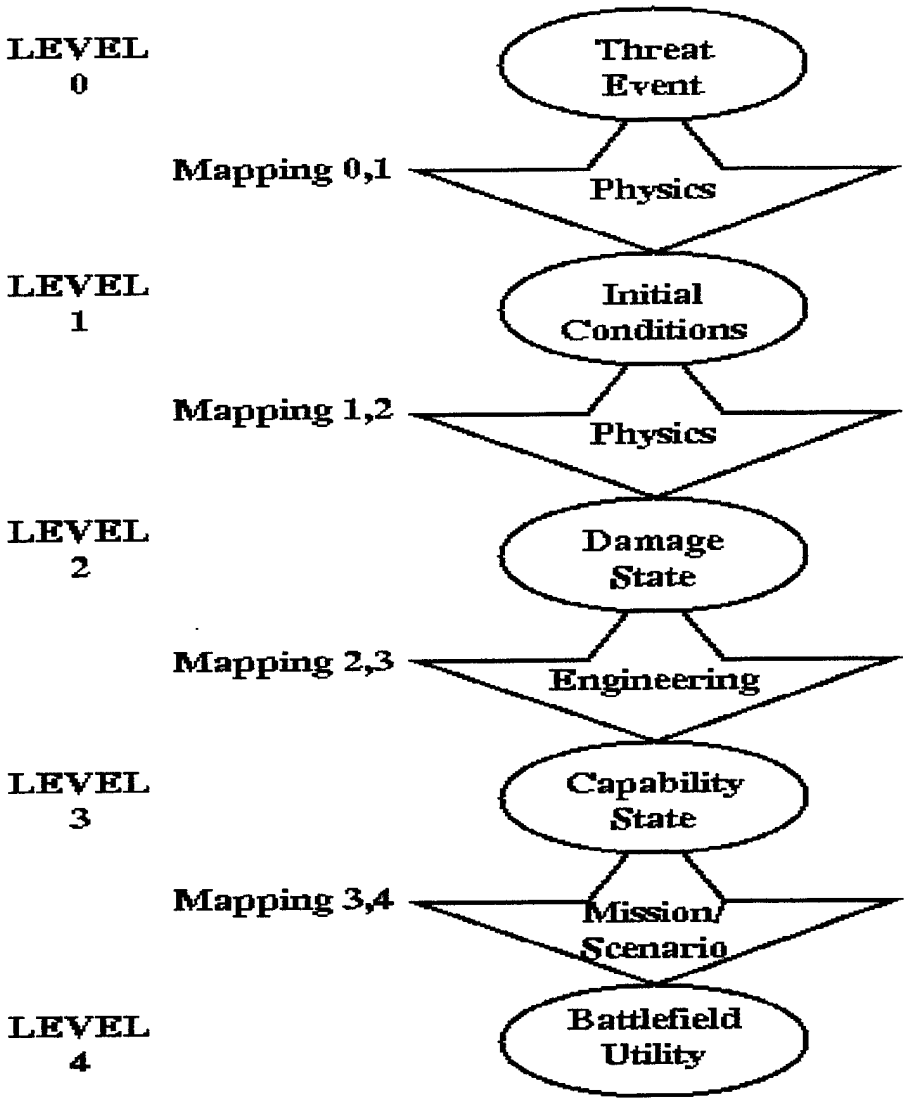

Figure 2. The V/L Taxonomy.

Figure 3 presents a wiring diagram that depicts the interconnections of the phases of an ISSA. The boxes shown internal to the larger boxes are products of that particular phase of the analysis. The arrows that connect the phases show how products of one phase feed into the other phases and then permeate the entire process. Internal to the process, there exist multiple feedback loops that are not shown on the diagram. Also, each of these phases is further constructed of multiple phases and individually tailored for the system under analysis.

Table 1. The Five Phases of an ISSA

Phase Number	Phase Title
1	System Familiarization
2	System Design Analysis
3	Threat Definition and Assessment
4	Vulnerability Assessment
5	Protection Assessment and Recommendations

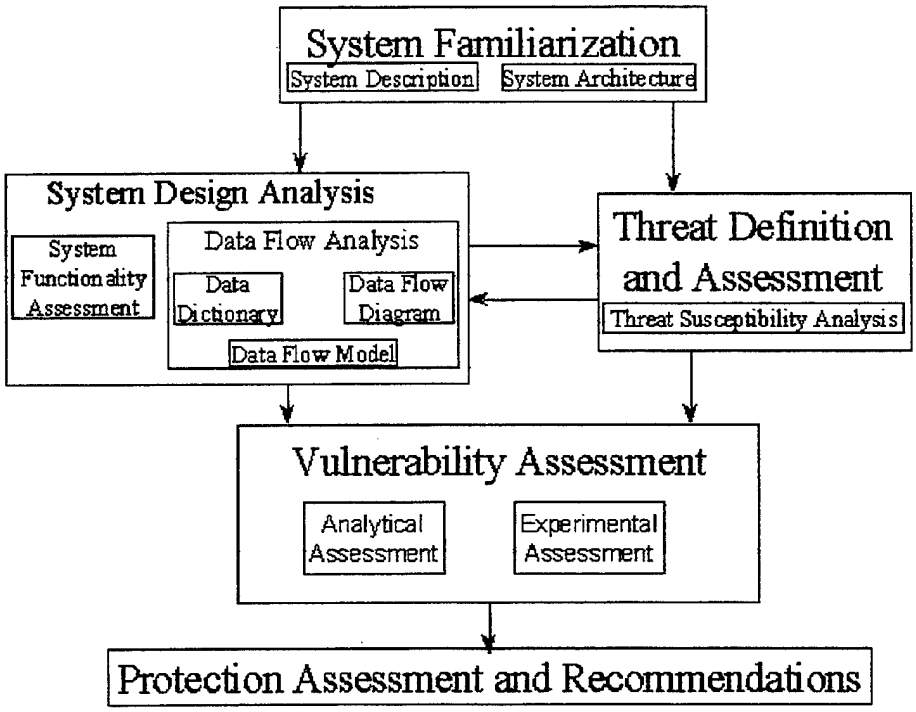

Figure 3. Schematic of the Methodology Flow of an ISSA.

In an ISSA, a system is made up of both hardware and software. These pieces are further subdivided into components and subsystems. These are defined in zum Brunnen [22] as follows:

"The hardware is made up of components, subsystems, and systems. A component is an individual item such as an integrated circuit (IC) chip, cable, disk platter, cooling-fan blade, printed circuit board, etc. A subsystem is an assemblage of components or subsystems. For example, a disk drive is a subsystem; it is constructed from motors, read/write heads, disk platters, cables, IC chips, printed circuit cards, etc. To further complicate matters, a disk drive is a component of an input/output (I/O) subsystem. An I/O subsystem is made up of disk drives, printed circuit cards, IC chips, cables, data buses, etc. A system is a collection of subsystems. Examples of subsystems are I/O, graphics, memory, power, etc."

2.1 The System Familiarization Phase. The system familiarization work will encompass a review of system documentation, as well as discussions with the program manager (PM) office and its contractors to gain knowledge or data concerning the system's mission critical INFOSYS resources, both hardware and software. System documentation, including the required operational capability (ROC), test and evaluation master plan (TEMP), operational requirements document (ORD), prime item development specification (PIDS), and software requirements specifications (SRS), will be reviewed to assimilate the various mission-critical INFOSYS resources into a single document.

An analysis of the system hardware will include the processors, data storage, I/O, and interconnections between the subsystems, as well as the system and other external interfaces. This analysis will be documented as the system architecture portion of the system familiarization phase. The analysis of system software will include understanding operating systems, network, and application programs. An overview of what information is used, where it is used, and how it flows will be developed and documented. This analysis will be documented as the system description portion of the system familiarization phase.

2.2 The System Design Analysis Phase. As shown in Figure 3, this phase has two major subcomponents: the system functionality assessment and the data flow analysis.

2.2.1 The System Functionality Assessment. As the name implies, this is an assessment of the functionality of the system. This assessment is done from the INFOSYS perspective and focuses on the mission-critical INFOSYS of the system. The goal of the functionality assessment is to

determine if the system can achieve its specific requirements from an INFOSYS perspective. In this assessment, the system requirements and specifications are mapped into the system description and system architecture produced in the system familiarization phase of the ISSA. This is an effort to determine if the requirements and specifications laid out by the system proponent are functionality obtainable by the designed system. This effort focuses on the INFOSYS components of the system and is not concerned with items such as ballistic protection, soldier compatibility, etc.

2.2.2 The Data Flow Analysis. This overview will be used to formulate the detailed program specifications for an information flow model (IFM) of the system under analysis. These specifications will be based on the system hardware, software, operating systems, protocols, topology, and interconnections between both internal subsystems and external communications. This phase of the ISSA uses all the products of the previous phases. The system description, system architecture, and system design assessment all bring critical information into this phase. An attempt will be made to reflect the system security policy and how it is enforced. The IFM is meant to provide some initial analytical measure of performance of the system for different configurations and scenarios. Possible reported performance metrics may include message latency and error rates vs. network load.

The data flow diagram generated will be documented. This documentation will be in the form of a data dictionary and transform descriptions. The data dictionary documents each of the interface flows and data stores on any data flow diagram. The transform descriptions document the internals of the data flow diagram processes in a rigorous fashion (usually through the use of structured English, decision tables, and decision trees). For further details on data flow diagrams, data dictionaries, and transform descriptions, see DeMarco [23].

The data flow diagram will be developed into a simulation using available modeling tools (e.g., an operational network [OPNET] simulation). This simulation will allow the behavior of the system's data flow through hardware components, software components, protocols, and interfaces to be studied in detail.

2.3 The Threat Definition and Assessment Phase. The System Threat Assessment Report (STAR) for the system will be reviewed for inclusion of current and future I/O specific threats, their mechanisms, or procedures. All available and relevant sources of threat information will be utilized during this threat definition phase. Relevant information will be leveraged to the greatest extent possible. To include both traditional and nontraditional sources (e.g., Federal Bureau of Investigation [FBI], National Security Agency [NSA], Defense Intelligence Agency [DIA], Computer Emergency Response Teams [CERTs], Central Intelligence Agency [CIA], bulletin boards, Hacker publications, etc.). The system's INFOSYS environments, from manufacturing, storage at the depot and on to deployment, will also be addressed during this investigation. The classes of possible threats are defined as:

- destruction of the system,
- interruption of service,
- removal or loss of information,
- disclosure of sensitive or classified information, and
- information corruption.

The threat assessment phase is critical in supporting the PM by ensuring that only relevant threats are included in the ISSA. An update to the STAR will be accomplished by working with the appropriate threat working groups to ensure that relevant I/O threats are considered and understood. One of the products of the threat definition and assessment will be a threat susceptibility analysis. In this analysis, both the likelihood of occurrence of a given threat and the potential susceptibility of the INFOSYS components of the system need to be determined. The threats to which the system has been determined to be susceptible are then reexamined, and the individual threat functioning mechanisms are analytically "played" against the information flow model specification (list of equipment, connections, etc.) that was made during the system familiarization phase of this ISSA. The result of this analytical play become one element of the vulnerability assessment. Only threats to which the system component(s) are susceptible need to be considered in further vulnerability assessments.

2.4 The Vulnerability Assessment Phase. The vulnerability assessment phase is broken into two pieces:

(1) analytical and

(2) experimental.

2.4.1 The Analytical Vulnerability Assessment. Given the combined use of the system description and architecture, the system design assessment, and the threat definition and susceptibility analysis, an analytical list of causes and effects are generated.

Consider the following example:

- within system C, if protocol X is used to send a particular packet of size E bits from component A to component B, and
- if the packet receive buffer in component B is of size D bits, and
- if D (the buffer size in bits) is smaller than E (the packet length in bits) or $D < E$.

The resulting event (in the case of this example, buffer overflow) can be predicted. With some degree of experience the analyst can than predict the result of this event (in this example, buffer overflow), the likelihood of this event, and the degree to which it could possibly affect the ability of the system to complete its mission.

2.4.2 The Experimental Vulnerability Assessment. The system (as constructed in the I/O laboratory, either real or surrogate) is then subjected to a suite of laboratory experiments that is modeled after the prioritized list vulnerabilities generated in the analytical portion of this phase. The predicted results of the analytical portion will then be either confirmed or negated.

The laboratory experiments will also yield data upon which I/O algorithms can be based. These algorithms will then be incorporated into the data flow modeling of the system being done in the

system design analysis portion of the ISSA. The algorithms and resulting models are then added to the common library of data flow tools for use in future ISSAs.

2.4.3 Vulnerability Assessments in General. The methodology used in the assessment must be robust enough to adequately address the balance between the equally important component vulnerabilities: the likelihood of occurrence and the effectiveness severity given this occurrence. This balance can be achieved by taking a product of these two probabilities. One method of performing an assessment is detailed in Guzie [24]. The probabilities of occurrence used here were previously determined during the threat assessment and definition phase of the ISSA. The determination of effectiveness severity, given the occurrence of the threat, is the bulk of the effort during this phase.

Software issues focus on threats that originate in software. Generally, software threats can be lumped into two categories: accidental and malicious. When damage occurs by accident, the code involved is termed a software bug. This bug may have been caused by programmer error, the resulting actions of the bug were totally unintentional. Bugs are perhaps the most common cause of unexpected program behavior.

Opposed to the unintentional results of software bugs are the intentional results of the malicious codes or programmed threats. These threats are built with deliberate instructions by individuals who intend for abnormal, and often damaging, behavior to occur.

Two of the many potential risks that require assessment during an ISSA are those from threats posed by malicious codes and hostile intrusions. It needs to be noted that an ISSA is not limited only to threats from malicious codes and hostile intrusions. These two threats cut across many of the system properties that are assessed in an ISSA. Namely, these are system integrity, system availability, system confidentiality, authorization and accountability of systems and users, data integrity, data availability, data confidentiality, and functional correctness.

2.5 The Protection Assessment and Recommendations Phase. This is an effort to formally present measures that may be taken to protect the system under analysis from the potential threats identified during the threat definition and assessment phase. These measures may include items such as developed or modified malicious code or intrusion indications and warnings devices or software (these are I/O tools) configured for the system. The validation and verification for the proper utilization of these tools (devices or software) is done by installing them on the system (real or surrogate) as configured in the I/O laboratory and applying the predicted threats to the system.

3. The Relationship of the ISSA Process to the V/L Taxonomy

Throughout the individual phases of an ISSA, the behavior or state of various INFOSYS properties are analyzed. Table 2 presents the definitions of these various properties as per VAL-CE-TR-92-22 [3].

As previously stated, the V/L taxonomy is the guide used by SLAD for integrated analyses. The V/L taxonomy presents a structured approach for taking threat effects and progressing through a series of mappings to produce a platform battlefield utility. This structure is shown in Figure 2.

The threats of concern in an ISSA is I/O based. Therefore, one of the purposes of an ISSA is to map the effects resulting from an I/O-based threat event to a platform battlefield utility. The mappings will primarily be functions of computer science (e.g., network theory, computer engineering, etc.), communications, and electronics. The individual component level effects will primarily be seen as computer science types of effects. These component level effects will further cause effects as a result of networking and communications within the platform (or system). Table 3 presents a sample breakout of INFOSYS-related metrics (properties that can be measured) as a function of V/L taxonomy level. The example metrics used in Table 3, for V/L taxonomy levels 2 and 3, are the various INFOSYS properties that are presented in Table 2.

Table 2. Various INFOSYS Properties and Definitions

Property	Definition
System Integrity	The system's ability to prevent malicious (and, to some extent, accidental) effects on the hardware, system software, and intercommunications.
System Availability	The system's ability to prevent system and communication outages, including temporary unavailability of resources. Such outages may include malicious or accidental denials of system service.
System Confidentiality	The system's ability to prevent the undesired dissemination or acquisition of sensitive system code or data, particularly if the application can be compromised; otherwise, for example, knowledge of the system design, a specific algorithm, a piece of code, a password, a cryptographic key, a network authenticator, or a piece of equipment could lead to a system subversion.
Authorization and Accountability of Systems and Users	A system's is capability to control which subsystems and individuals are using it; otherwise, it may be vulnerable to spoofing attacks, penetrations, and other forms of misuse. After any such attack, the system's inability to provide real-time (or at least rapid) accountability and audit-trail analysis may lead to additional compromises of survivability.
Data Integrity	The system's ability to prevent undesired alteration of input data, internal stored data, or output data. Data integrity includes internal data consistency (particularly important in a highly dispersed environment), as well as external consistency with the real world.
Data Availability	The system's ability to prevent disruption in timely access to data, including sensor data in a control system. Multiple versions of critical data and alternative sensors can help increase data availability.
Data Confidentiality	The system's ability to prevent undesired data disclosure. For example, a penetrator could obtain sensitive data that would compromise the application's ability to fulfill its requirements.
Fault Tolerance	The system's ability to prevent undesired effects resulting from failure of underlying hardware components, subsystems, or indeed the entire system. Essentially, fault tolerance is both a system integrity issue and a system reliability issue. Constructive use of redundancy is essential. Survivability is a particular concern when the nominal fault tolerance coverage is expected.

Table 2. Various INFOSYS Properties and Definitions (continued)

Property	Definition
Functional Correctness	Assurance that a flaw in the application or in the computer operating system or a human error in system maintenance cannot compromise the application. Good software engineering, development practices, and system operation are important but are clearly not enough by themselves.
Real-Time Availability	Assurance that the real-time processing can be done in a timely way, and that the system is protected against maliciously or accidently caused delays. This property includes the real-time availability of the system, data, and other resources.
Real-Time accountability	Such as anomaly detection and audit-trail analysis.
Timely Detection and Correction of Deviant System Behavior	The ability of the system to reconfigure itself in the face of nontolerated faults or penetrations. Recovery from serious outages may or may not be allowed to incur long time delays or human intervention. In cases where human intervention is not possible, thorough advanced planning is necessary.
Functional Timeliness	Such as strict bounds in hard real-time systems or best-effort intentions in fuzzy real-time systems.
Ability to Maintain Minimum Essential System Requirements	The system's ability to conduct operations in the presence of unforeseen adverse conditions. This also involves the establishment of the minimum operating requirements. The user of the system generates these requirements based on the minimum system functionality needed to complete mission requirements.

One of the goals of SLAD's I/O mission area is to robustly address the class of questions such as the following.

- How does data integrity (at V/L level 2) relate to reliability (at V/L level 3)?

- Given this relationship, how then does reliability (at V/L level 3) relate to acquisition (at V/L level 4)?

Table 3. A Sample Breakout of INFOSYS-Related Metrics to V/L Taxonomy Levels

V/L Taxonomy Level	Example Metrics[a]
Sample Level 2 Metrics (Damage States) [System, Subsystem, or Component]	• System integrity • System availability • System confidentiality • Authorization and accountability of systems and users • Data integrity • Data availability • Data confidentiality • Fault tolerance • Functional correctness • Real-time availability • Real-time accountability
Sample Level 3 Metrics (Capability States) [System, Subsystem, or Component]	• Timely detection and correction of deviant system behavior • Functional timeliness • Ability to maintain minimum essential system requirements • Reliability • Maintainability • Supportability • Range and accuracy • Speed of performance
Sample Level 4 Metrics (Battlefield Utility) [Platform]	• Mobility • Firepower • Acquisition • Crew • Communication • Other

[a] Here, the term "System" refers to "Information Systems."

The interrelationships between the properties (or metrics) are nontrivial and require a large consolidated effort to understand, analyze, and model.

4. Summary

The system ISSA plan is a focused plan to provide the decision makers with the necessary information with which make informed decisions concerning the vulnerabilities and susceptibilities

of the system to I/O threats. The associated research and analyses are performed by a team of people who are knowledgeable in the various required I/O areas.

The multiple phases of the effort should not be considered separate, stand-alone tasks. These phases are intertwining tasks. Each of these tasks depends upon the others. For example, during the system familiarization phase, the specifics that will drive the IFM specifications are determined (i.e., the identification of the specific types of machines, network modules, physical configurations, and particular protocols used in the system). These same specifics will determine some of the particular threat susceptibilities examined in the threat assessment and definition phase.

The system design analysis phase will clarify questions that come up during the system familiarization phase and will feed the threat assessment and definition phase. As an example, how is module A connected to module B (cable and connector type, etc.), what communications protocols are used to manage this link, and what is the data transmission rate of this link. While there are separate phases of work being discussed, in practical application, they are a single, large, interconnected effort.

The system ISSA will identify, specify, and inform decision makers of the system's vulnerabilities to I/O-based threats. Protection measures will be recommended to identify and minimize the impact on system performance. The plan is formulated in various phases to help the decision makers modify the necessary hardware and software within the program cycle to meet the necessary survivability requirements. By addressing the I/O threats, the system will significantly improve its survivability by planning for both the avoiding and withstanding of potential problems with I/O-based threats. Avoiding these problems will allow the system to effectively contribute during combat on the future battlefield.

INTENTIONALLY LEFT BLANK.

5. References

1. Joint Pub 6-0. "Doctrine for Command, Control, Communications, and Computers (C^4) Systems Support to Joint Operations." 3 June 1992.

2. U.S. Department of the Army. "Information Operations." FM 100-6. August 1996.

3. Barnes, A. L., A. P. Hollway, and P. G. Neumann. "Survivable Computer-Communication Systems." VAL-CE-TR-92-22, U.S. Army Vulnerability Assessment Laboratory, May 1993.

4. Pressman, R. S. "Software Engineering - A Practitioner's Approach." ISBN 0-07-050814-3, Third Edition, McGraw-Hill, Inc., 1992.

5. Deitz, P. H. "Comments by the BRL in Response to the Report of the Board on Army Science and Technology's Committee on Vulnerability Analysis." U.S. Army Ballistic Research Laboratory, Aberdeen Proving Ground, MD, unpublished.

6. Deitz, P. H., and A. Ozolins. "Computer Simulations of the Abrams Live-Fire Testing." BRL-MR-3755, U.S. Army Ballistic Research Laboratory, Aberdeen Proving Ground, MD, May 1989.

7. Abell, J. M., L. K. Roach, and M. W. Starks. "Degraded States Vulnerability Analysis." BRL-TR-3010, U.S. Army Ballistic Research Laboratory, Aberdeen Proving Ground, MD, June 1989.

8. Abell, J. M., M. D. Burdeshaw, and B. A. Rickter. "Degraded States Vulnerability Analysis: Phase II." BRL-TR-3161, U.S. Army Ballistic Research Laboratory, Aberdeen Proving Ground, MD, October 1990.

9. Deitz, P. H., M. W. Starks, J. H. Smith, and A. Ozolins. "Current Simulation Methods in Military Systems Vulnerability Assessment." BRL-MR-3880, U.S. Army Ballistic Research Laboratory, Aberdeen Proving Ground, MD, November 1990.

10. Starks, M. W. "Improved Metrics for Personnel Vulnerability Analysis." BRL-MR-3908, U.S. Army Ballistic Research Laboratory, Aberdeen Proving Ground, MD, May 1991.

11. Klopcic, J. T., M. W. Starks, and J. N. Walbert. "A Taxonomy for the Vulnerability/Lethality Analysis Process." BRL-MR-3972, U.S. Army Ballistic Research Laboratory, Aberdeen Proving Ground, MD, May 1992.

12. Roach, L. K. "Fault Tree Analysis and Extensions of the V/L Process Structure." ARL-TR-149, U.S. Army Research Laboratory, Aberdeen Proving Ground, MD, June 1993.

13. Ozolins, A. "Vulnerability of Approximate Targets." ARL-TR-154, U.S. Army Research Laboratory, Aberdeen Proving Ground, MD, June 1993.

14. Walbert, J. N., L. K. Roach, and M. D. Burdeshaw. "Current Directions in the Vulnerability/Lethality Process Structure." ARL-TR-296, U.S. Army Research Laboratory, Aberdeen Proving Ground, MD, October 1993.

15. Walbert, J. N. "The Mathematical Structure of the Vulnerability Spaces." ARL-TR-634, U.S. Army Research Laboratory, Aberdeen Proving Ground, MD, November 1994.

16. zum Brunnen, R. L. "Introducing Chemical/Biological Effects Into the Ballistic Vulnerability/Lethality Taxonomy." ARL-TR-715, U.S. Army Research Laboratory, Aberdeen Proving Ground, MD, March 1995 (On the World Wide Web at http://ftp.arl.mil/~rick/reports/arl715.html).

17. Mar, M. H. "Electromagnetic Pulse (EMP) Coupling Codes for Use With the Vulnerability/Lethality Taxonomy." ARL-TR-786, U.S. Army Research Laboratory, Aberdeen Proving Ground, MD, July 1995.

18. Ruth, B. G., and M. H. Mar. "High-Altitude Electromagnetic Pulse (HEMP) Analysis of a Generic Communications Network Switching Node Using the Nuclear Electromagnetic Pulse (EMP) Vulnerability/Lethality Taxonomy." ARL-TR-888, U.S. Army Research Laboratory, Aberdeen Proving Ground, MD, October 1995.

19. zum Brunnen, R. L., R. W. Kunkel, Jr., and J. G. Reza. "Target Description Specifications for the Conduct of Integrated Analysis." ARL-TR-1071 (also at http://ftp.arl.mil/~rick/reports/arl1071.html), U.S. Army Research Laboratory, Aberdeen Proving Ground, MD, April 1996.

20. Ruth, B. G., and P. J. Hanes. "A Time-Discrete Vulnerability/Lethality Process Structure." ARL-TR-1222, U.S. Army Research Laboratory, Aberdeen Proving Ground, MD, November 1996.

21. Roach, L. K. "The New Degraded States Vulnerability Methodology (DSVM): A Change in Philosophy and Approach." ARL-TR-1223, U.S. Army Research Laboratory, Aberdeen Proving Ground, MD, November 1996.

22. zum Brunnen, R. L. "Real World Computing Model for Information Systems Survivability Assessments." Draft technical report, U.S. Army Research Laboratory, Aberdeen Proving Ground, MD, March 1998.

23. DeMarco, T. "Structured Analysis and System Specification." Yourdon Press, 1979.

24. Guzie, G. L. "The Application of Risk Assessment Theory to Countermeasure Vulnerability Assessment." Draft technical report, U.S. Army Research Laboratory, Aberdeen Proving Ground, MD, January 1996.

NO. OF COPIES ORGANIZATION

2 DEFENSE TECHNICAL INFORMATION CENTER
DTIC DDA
8725 JOHN J KINGMAN RD
STE 0944
FT BELVOIR VA 22060-6218

1 HQDA
DAMO FDQ
DENNIS SCHMIDT
400 ARMY PENTAGON
WASHINGTON DC 20310-0460

1 DPTY ASSIST SCY FOR R&T
SARD TT F MILTON
RM 3EA79 THE PENTAGON
WASHINGTON DC 20310-0103

1 OSD
OUSD(A&T)/ODDDR&E(R)
R J TREW
THE PENTAGON
WASHINGTON DC 20301-7100

1 CECOM
SP & TRRSTRL COMMCTN DIV
AMSEL RD ST MC M
H SOICHER
FT MONMOUTH NJ 07703-5203

1 PRIN DPTY FOR TCHNLGY HQ
US ARMY MATCOM
AMCDCG T
M FISETTE
5001 EISENHOWER AVE
ALEXANDRIA VA 22333-0001

1 DPTY CG FOR RDE HQ
US ARMY MATCOM
AMCRD
BG BEAUCHAMP
5001 EISENHOWER AVE
ALEXANDRIA VA 22333-0001

1 INST FOR ADVNCD TCHNLGY
THE UNIV OF TEXAS AT AUSTIN
PO BOX 202797
AUSTIN TX 78720-2797

NO. OF COPIES ORGANIZATION

1 GPS JOINT PROG OFC DIR
COL J CLAY
2435 VELA WAY STE 1613
LOS ANGELES AFB CA 90245-5500

3 DARPA
L STOTTS
J PENNELLA
B KASPAR
3701 N FAIRFAX DR
ARLINGTON VA 22203-1714

1 US MILITARY ACADEMY
MATH SCI CTR OF EXCELLENCE
DEPT OF MATHEMATICAL SCI
MDN A MAJ DON ENGEN
THAYER HALL
WEST POINT NY 10996-1786

1 DIRECTOR
US ARMY RESEARCH LAB
AMSRL CS AL TP
2800 POWDER MILL RD
ADELPHI MD 20783-1145

1 DIRECTOR
US ARMY RESEARCH LAB
AMSRL CS AL TA
2800 POWDER MILL RD
ADELPHI MD 20783-1145

3 DIRECTOR
US ARMY RESEARCH LAB
AMSRL CI LL
2800 POWDER MILL RD
ADELPHI MD 20783-1145

ABERDEEN PROVING GROUND

4 DIR USARL
AMSRL CI LP (305)

NO. OF COPIES	ORGANIZATION
1	OUSD AT STRT TAC SYS DR SCHNEITER RM 3E130 3090 DEFENSE PENTAGON WASHINGTON DC 20310-3090
1	OASD C31 DR SOOS RM 3E194 6000 DEFENSE PENTAGON WASHINGTON DC 20301-6000
1	UNDER SEC OF THE ARMY DUSA OR ROOM 2E660 102 ARMY PENTAGON WASHINGTON DC 20310-0102
1	ASST SECY ARMY RESEARCH DEVELOPMENT ACQUISITION SARD ZD ROOM 2E673 103 ARMY PENTAGON WASHINGTON DC 20310-0103
1	ASST SECY ARMY RESEARCH DEVELOPMENT ACQUISITION SARD ZP ROOM 2E661 103 ARMY PENTAGON WASHINGTON DC 20310-0103
1	ASST SECY ARMY RESEARCH DEVELOPMENT ACQUISITION SARD ZS ROOM 3E448 103 ARMY PENTAGON WASHINGTON DC 20310-0103
1	OADCSOPS FORCE DEV DIR DAMO FDZ ROOM 3A522 460 ARMY PENTAGON WASHINGTON DC 20310-0460
1	OADCSOPS FORCE DEV DIR DAMO FDW RM 3C630 460 ARMY PENTAGON WASHINGTON DC 20310-0460

NO. OF COPIES	ORGANIZATION
1	HQ USAMC DEP CHF OF STAFF FOR RDA AMCRD 5001 EISENHOWER AVE ALEXANDRIA VA 22333-0001
1	ARMY TRNG & DOCTRINE COM ATCD B FT MONROE VA 23561-5000
1	ARMY TRADOC ANL CTR ATRC W MR KEINTZ WSMR NM 88002-5502
1	ARMY RESEARCH LABORATORY AMSRL SL PLANS AND PGMS MGR WSMR NM 88002-5513
1	ARMY RESEARCH LABORATORY AMSRL SL E MR SHELBURNE WSMR NM 88002-5513
1	ARMY RESEARCH LABORATORY AMSRL ST DR ROCCHIO 2800 POWDER MILL RD ADELPHI MD 20783-1197

NO. OF
COPIES ORGANIZATION

ABERDEEN PROVING GROUND

1 ARMY TEST EVAL COM
AMSTE TA
APG MD 21005-5055

1 US ARMY EVAL ANALYSIS CTR
CSTE EAC MR HUGHES
4120 SUSQUEHANNA AVE
APG MD 21005-3013

1 US ARMY EVAL ANALYSIS CTR
CSTE EAC SV DR HASKELL
4120 SUSQUEHANNA AVE
APG MD 21005-3013

1 ARMY RESEARCH LABORATORY
AMSRL SL
DR WADE
APG MD 21005-5068

2 ARMY RESEARCH LABORATORY
AMSRL SL B
MS SMITH
W WINNER
APG MD 21005-5068

1 ARMY RESEARCH LABORATORY
AMSRL SL E
DR STARKS
APG EA MD 21010-5423

NO. OF COPIES	ORGANIZATION
2	DIR ARL AMSRL IS DR GANTT LTC WALCZAK 2800 POWDER MILL RD ADELPHI MD 20783-1197
4	DIR ARL AMSRL SL EI A L BARNES J LURSKI C J MEINCKE J NOWAK FORT MONMOUTH NJ 07703-5602
18	DIR ARL AMSRL SL EA MR FLORES MR LANDIN MR STAY AMSRL SL EI MS CHRISTIANSON SGT GOWINS MS JIMENEZ MR MAREZ MR MCDONALD MR SWEARINGEN CPT(P) THEODOSS MR WILLIAMS AMSRL SL EM C A OCHOA JR J PALOMO AMSRL SL ET MS THOMPSON DR YEE AMSRL SL EV MR LUJAN DR MORRISON MR SPEZIALE WHITE SANDS MISSILE RANGE NM 88002-5513
1	CDR INSCOM LIWA MS MEHAN 8825 BEULAH ST FORT BELVOIR VA 22060-5246
1	CDR NGIC AING SBE MR TERRY 220 SEVENTH ST NE CHARLOTTESVILLE VA 22902-5396
1	US MIL ACADEMY B MALONEY WEST POINT NY 10996

NO. OF COPIES	ORGANIZATION
	ABERDEEN PROVING GROUND
1	CDR USAEAC CSTE EAC SV MR MYERS 4120 SUSQUEHANNA AVE
40	DIR ARL AMSRL SL B, R S SANDMEYER AMSRL SL BA, M E RITONDO E M VOGEL AMSRL SL BE, D C BELY D W PETTY AMSRL SL BG, J J FRANZ P J KUSS J C LIU J J PLOSKONKA A L YOUNG R N ZIGLER AMSRL SL BN, D B FARENWALD AMSRL SL EI, E J PANUSKA R L ZUM BRUNNEN (25 CPS) AMSRL SL EM, J J FEENEY AMSRL SL ET, D W BAYLOR

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	August 1998	Final, September 1997 - March 1998

4. TITLE AND SUBTITLE
The Methodology Process Flow of a SLAD Information Systems Survivability Assessment

5. FUNDING NUMBERS
8LEH40

6. AUTHOR(S)
Richard L. zum Brunnen

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
U.S. Army Research Laboratory
ATTN: AMSRL-SL-EI
Aberdeen Proving Ground, MD 21010-5423

8. PERFORMING ORGANIZATION REPORT NUMBER
ARL-TR-1747

9. SPONSORING/MONITORING AGENCY NAMES(S) AND ADDRESS(ES)

10.SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution is unlimited.

12b. DISTRIBUTION CODE

13. ABSTRACT *(Maximum 200 words)*

The Information Systems Survivability Assessment (ISSA) is a process of analytical steps that the Survivability/Lethality Analysis Directorate (SLAD) of the U.S. Army Research Laboratory (ARL) applies to networked Automated Information Systems (INFOSYS) of military interest.

The ISSA Plan for a particular system is a focused plan that has been designed to provide the decision-makers the necessary information with which to make informed decisions concerning the vulnerabilities and susceptibilities of the system to Information Operations (IO) threats. The ISSA is a multiple-phase effort; these phases are intertwining tasks. Each of these tasks depends upon the others.

The plan is formulated in various phases to help the decision-makers modify the necessary hardware and software within the program cycle to meet the necessary survivability requirements. The ISSA culminates with protection measures being recommended to identify and minimize the impact of the IO threats on system performance. By addressing the IO threats, the system will significantly improve its survivability by planning for both the avoiding and withstanding of potential problems with IO-based threats.

This report discusses the ISSA process in detail and shows how each small task dovetails into the larger effort.

14. SUBJECT TERMS	15. NUMBER OF PAGES
information systems survivability, information operations, information warfare, assessment, methodology	26
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	UL

INTENTIONALLY LEFT BLANK.

USER EVALUATION SHEET/CHANGE OF ADDRESS

This Laboratory undertakes a continuing effort to improve the quality of the reports it publishes. Your comments/answers to the items/questions below will aid us in our efforts.

1. ARL Report Number/Author ARL-TR-1747 (zum Brunnen) Date of Report August 1998

2. Date Report Received _____

3. Does this report satisfy a need? (Comment on purpose, related project, or other area of interest for which the report will be used.) _____

4. Specifically, how is the report being used? (Information source, design data, procedure, source of ideas, etc.) _____

5. Has the information in this report led to any quantitative savings as far as man-hours or dollars saved, operating costs avoided, or efficiencies achieved, etc? If so, please elaborate. _____

6. General Comments. What do you think should be changed to improve future reports? (Indicate changes to organization, technical content, format, etc.) _____

CURRENT ADDRESS

_____
Organization

_____
Name E-mail Name

_____
Street or P.O. Box No.

_____
City, State, Zip Code

7. If indicating a Change of Address or Address Correction, please provide the Current or Correct address above and the Old or Incorrect address below.

OLD ADDRESS

_____
Organization

_____
Name

_____
Street or P.O. Box No.

_____
City, State, Zip Code

(Remove this sheet, fold as indicated, tape closed, and mail.)
(DO NOT STAPLE)